

FIG. 1

```
[Device Driver 1: installs wrapper]
    dd1_old = services[ CREATE_PROCESS_INDEX ];
    services[ CREATE_PROCESS_INDEX ] = dd1_new;
```

```
[Device Driver 2: installs wrapper]
    dd2_old = services[ CREATE_PROCESS_INDEX ];
    services[ CREATE_PROCESS_INDEX ] = dd2_new;
```

```
[Device Driver 1: removes wrapper]
    services[ CREATE_PROCESS_INDEX ] = dd1_old;
```

Notice that services[CREATE_PROCESS_INDEX] now contains its original value (that of the real System Service). Device Driver 2 has been unwrapped without its knowledge!

FIG. 2

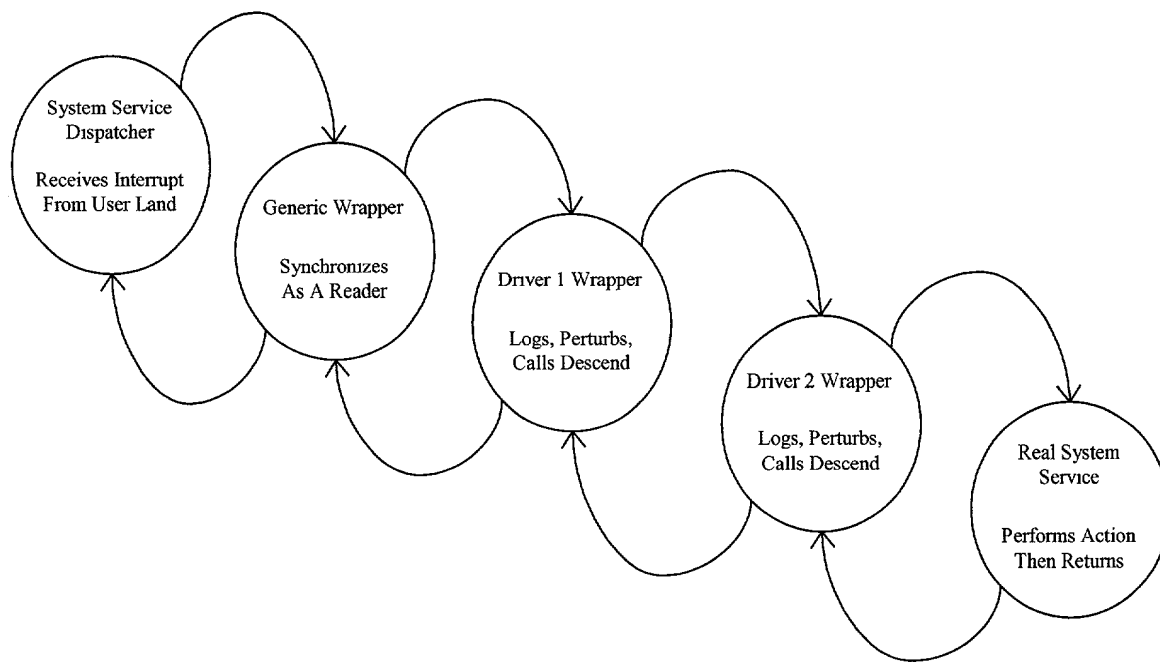


FIG. 3